Building a Security Metrics Program
Transcript

Part 1: Understand Your Objectives and the Business Context

Julia Allen: Welcome to CERT's podcasts series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Melon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and executive outreach. Today I'm very pleased to introduce Betsy Nichols, Chief Technology Officer at PlexLogic and a faculty member at the Institute for Applied Network Security. Today we'll be discussing how to develop and sustain
an effective security metrics program. So welcome Betsy. Thanks for being withus today.

Betsy Nichols: Well thank you. I'm delighted to be here.

Julia Allen: So to get the ball rolling, why do you think the security community struggles so much with being able to define, collect, and present security metrics? Why is this such a tough subject?

Betsy Nichols: Well certainly this is something I hear all the time that people say that they struggle with security metrics and I think there're probably two primarily sources of difficulty. They have to do with "the what" and "the how" basically. So let me talk first about "the what." "The what" means what you really need is a really clear statement of objectives for measuring and providing whatever enlightenment those metrics are going to deliver. "The how" is more along the lines of creating tools for automation so that metrics have repeatability, clarity, and authority.

Looking at the first topic of "the what," in security metrics we have yet to really converge on a clear statement of objectives I think. I mean what specific enlightenment do we want? If you look at other disciplines – disciplines like data center service level agreements are an example – the classic metrics that are used there are mean time between failure (MTBF), mean time to repair (MTTR), availability, response time. These are metrics that the industry has converged on as being useful. And what are they doing? They're trying to characterize, in the case of MTBF (mean time between failures) is frequency of failures. In the case of MTTR (or the mean time to repair), that's duration of failures once they do occur. Availability is just the probability that a user when he wants to access a service can indeed access it. Response time has to do with the quality of service that he gets once he can access it.

Those are all topics that an industry has converged upon, that says these things need to be measured and they need to monitored carefully. And these are the agreed-upon measurements that we're going to use. To just take analogies from healthcare, you get blood pressure, temperature, height, weight, pulse rate, things like that. Again what we're trying to do is focus on a specific aspect of, in this case, an individual's current medical condition.

Julia Allen: In that particular example, you have the number and then you have either the meaning ascribed to the number or how a particular number or metric is used in concert with others to derive meaning, right?

Betsy Nichols: Yes, yes typically metrics such as these have what you might call either a baseline or goal. In service level agreements for example, you have the desired levels that you want to achieve and the measurements are made in connection with those. And there is a way to interpret when you don't make those levels, when you don't achieve those levels.

Julia Allen: So business leaders like numbers, right? So assuming we can define and collect them, do you think meaningful metrics particularly with respect to security are a useful way to get leaders to pay attention?

Betsy Nichols: Absolutely, I absolutely do. The problem is is that lots of times when leaders make a request for metrics or when the objective stated – it is so broad that it's almost impossible to achieve.

For example, it's not unusual that I hear chief information security officers (CISO) that I speak with say they get questions like "Are we secure? Are we spending too much?" – questions like that. Well those are very good questions; there's no question. But the point is is that in order to get a useful metric that can begin to address a question like that, it needs to be broken down into something more specific.

I think it's important for business leaders who like numbers to provide just a little bit more information to the people that are generating metrics so that they can provide metrics that have insight on specific topics, not something as general. It's like when you ask "Am I healthy?" I mean, it's almost an unanswerable question but what you can do is you can say "Is my blood pressure normal?" Now "Is my blood pressure normal?" is a question that would, may not be all that interesting to somebody who's 19 and hale and hardy but to somebody who is 70 years old and has hypertension, they may want to invest in a bunch of equipment so that they can measure that hourly if necessary.

Julia Allen: So in that, again, I like your healthcare analogy because it's something everybody can identify with. Again this notion of context, putting the question and the whatever like blood pressure, whatever you're collecting or reporting on. You gave a nice example of putting that in context so clearly that's very critical.

Betsy Nichols: Yes. So the context, mapping it to the business is another way that people often say essentially the same thing.

Part 2: Selecting Useful Metrics Based on Risk

Julia Allen: So you've given some great examples. Let's take this a little bit further. So how would I know, from a characteristic sense perhaps, how would I know a good metric if I saw one as contrasted with a bad one? It sure would be great if we could do better than high, medium, low or red, yellow, green.

Betsy Nichols: Yes, interesting. I know when I first started out trying to develop software that would automate metric collection, I resisted this red, green, yellow situation. I always wanted to be able to provide somebody a number or a score or anything that was sort of quantitative as opposed to the fuzzy red, green, yellow notion, and I got a lot of push back on that. I guess my conclusion from all of this is that we'll never get away from the red, green, yellow notion but you should think of that as something that's sort of an end product and that in order to get to that you need a lot of quantitative data.

So for example, let's take the situation where maybe you're in a retail company and wireless security of late has been a very topical subject. As a matter of fact there was a segment on "60 Minutes" not long ago about the TJX breach that led to unauthorized disclosure of credit card and Social Security information for over 90 million individuals. So this has gotten a lot of attention. Now what you may find is that your board of directors is saying, "What's the situation here? Are we going to have a '60 Minute' moment?" And it might be most efficient to communicate with them in terms of red, green, yellow. You set up targets and if you meet the target it's green, if you're not meeting it by very much it's yellow, and if you're not meeting it by a long shot it's red. And maybe that's the easiest way to convey in a 30 second timeframe where we stand with respect to wireless security. But beneath that, what you would like to be able to do is break that problem down into something that is a lot of smaller problems that are readily measurable.

Julia Allen: Right and it also occurs to me as you're breaking it down and also building it back up again to some more qualitative representation – this is where you get back to this whole notion that security is a risk management issue. That the determination of where these different metrics or measures fall, red, yellow, green if you will, have to do with the organization's risk tolerance. Is that what you see?

Betsy Nichols: Yes and as a matter of fact really in order to find out what defines a topical metric which is the best kind of metric in my opinion basically you leverage a risk analysis to do that.

Julia Allen: Can you tell us a little bit more about that?

Betsy Nichols: Yes, well essentially, a structured risk analysis – what it basically does is it identifies areas of unacceptably high risk. And a risk is typically identified as a four-tuple in my mind. When you look at most risk models, what it identifies is (1) the vulnerability, (2) a threat that exists against that vulnerability, (3) the impact if that threat is successful in exploiting the vulnerability, and (4) the value of the asset involved.

Those four things typically go into an identification of a risk and all of those four things can be, to some degree, measured. Certainly the existence of vulnerabilities can be measured. Severity of vulnerability can be assigned and typically is assigned by the vulnerability measurement and monitoring products that are out there.

So essentially what you can do is breakdown a risk to these four items and then those four items can be measured. How many assets do you have that are high value assets that have at the same time high value or high severity vulnerabilities with threats that are of high probability with large impact? You can essentially take the risk analysis and use that to inspire what metrics you want to focus on first.

Julia Allen: Well that's – that's great because that also gives you that additional piece of context tying back to the business objectives – what's important to keep the organization moving forward. So you can justify your security investments in those types of terms.

Betsy Nichols: Exactly, exactly.

Julia Allen: So you said that your favorite security metrics are topical. Can you say a little bit more about what you mean by that and maybe what some of your favorite metrics are even though we've said that you require context and other kinds of ties to the business, do you have some favorites?

Betsy Nichols: The first requirement for a good metric is that it be topical. The second requirement is that there be data to back it up and as I try to generate metrics from existing data, it certainly is becoming more and more obvious to me that metrics really are all about data.

But in terms of some specific metrics that I really like, I like the simple metric security budget as a percent of the overall IT budget. I think that's an interesting metric. It has the advantages that it's easy to understand. It's typically of high interest to executives. It has the disadvantage though that the definition of a security budget is fuzzy particularly as you cross enterprise boundaries. But if you have business units within the same organization and you can standardize on that definition, then that's a pretty interesting number.

Another interesting metric that I've talked to various CISOs about that is of interest is where the CISO fits in the organization as reflected by, let's say, hops to the CEO or perhaps the number of board appearances per year.

Julia Allen: So that can tell you – I mean I'm jumping ahead here – but that can actually tell you something about where the organization places its importance with respect to information security, right?

Betsy Nichols: Absolutely. So it's a great proxy so to speak for influence. The con of course is that it doesn't really eliminate cheap talk – people that put CISOs at high levels in order to appear good but then don't actually follow through.

Another set of metrics though I like are metrics that are essentially derived based upon administrative groupings. This would apply to any company that has multiple divisions and what you do is generate metrics for each of those divisions and allow those divisions to compare themselves with each other, not so much as a stick but more as a carrot. If you see one organization that's doing much better than the others then presumably the laggards can look to the leaders and learn and improve.

Julia Allen: Well and hopefully foster a little healthy competition, right?

Betsy Nichols: Yes and it does. It generally does and in most of the situations that I've seen it's been healthy. It has not been unhealthy at all.

Part 3: Challenges and Getting Started

Julia Allen: So what are some of the challenges that business leaders face when they want to get serious about developing and managing a security metrics program? I mean you've mentioned some of them already. Are there others that come to mind?

Betsy Nichols: Well of course leveraging any existing risk analysis work is important and often times that sort of work has not been done. So there's a challenge there to get the structure in place to be able to do a good risk analysis. The second issue I would mention is data. As I said earlier, metrics are all about data. And besides just general data quality issues, there's also the issue of data politics which can enter in where people just decide they don't want to share data and that's an unfortunate circumstance. Lots of times there's disagreement as to what data is authoritative for a particular subject and there are disagreements between various data sources about, for example, what business unit an individual belongs to if you're going to roll up numbers by business units.

So the challenges are around being able to do a good risk analysis, being able to identify authoritative sources of data that can be readily accessed. And then the last challenge that I'll mention I guess is putting in place a program that is formal – that has accountability, it has assigned people, it has tools that can be used to perpetuate it and sustain a metrics program so that over time you get good data that is consistently gathered and repeatable.

Julia Allen: How do you advise your clients and customers to kind of – maybe the first small steps for getting started? How do you get them headed in the right direction?

Betsy Nichols: Okay, typically what I do is I ask for a topic of great interest and then we take it from there. So in the case of a retail organization, I would ask them about their wireless configuration. And then we'd talk about, if that's a topic of interest to them, then we break it down into understanding what do they have? Do they know where all the assets are that are involved with wireless communication? Do they know how they're configured? And we begin to look at metrics that we can derive from that information.

Julia Allen: So it occurs to me when you pick a specific topic clearly you have a high likelihood of a short term win. In other words if you focus tightly enough on a problem they currently have, you can actually produce a result or some benefit fairly quickly. Is that right?

Betsy Nichols: Yes, typically, typically we can produce – I've produced results within two weeks. And what you want to do of course is produce something that's repeatable so that not only do they get their first measurement but let's say it's useful to understand progress on a monthly basis, then they would put something in place that would allow that to happen so that you get a monthly number, so you can see a trend.

Julia Allen: Right because sometimes the actual trend in the metric is more enlightening as you said earlier, can be more enlightening than an individual number, right?

Betsy Nichols: That's exactly right. Really absolute numbers are awfully, awfully hard to come by in most cases. So that typically if you can't say "I need to have, I need to achieve a level let's say of 99 percent conformance or compliance with something," what I can do is say at least that I'm improving it 10 percent per quarter or something like that.

Julia Allen: We've mentioned the connection to risk assessment, risk management, but what about the concept of putting your security metrics program in the same context or using the same set of processes that the organization is using for collecting other performance metrics or indicators? Have you seen some success there?

Betsy Nichols: Yes. I think there's another interesting connection with just general process management and metrics. Many of the companies that I've worked with have adopted the Capability Maturity Model from SEI and what they do is they measure the maturity of their processes based upon, among other things, how well instrumented they are.

So for example if somebody is wanting to understand let's say the connection between security flaws in software and security incidents in applications that that software implements then they need to have good instrumentation not only of their software development processes but they have to have good instrumentation of their incident response so that they can for example discern between security-related events and non-security-related events if they want to. So basically what is happening is that as people make their processes more mature, they're adding more instrumentation to those processes and that instrumentation then can be used to derive metrics.

Julia Allen: Well with the example that you just gave in terms of applications development and incident response, typically those are siloed within organizations so having an integrated process brings those areas together I think in a more meaningful way from a metrics point of view.

Betsy Nichols: Yes and that's another interesting technical characteristic of metrics is that the most interesting metrics tend to integrate multiple sources – correlate what's happening in one place with another place. And so from a implementation perspective any automation system needs to be really good at data integration.

Julia Allen: Well Betsy this has just been fabulous in terms of I think in giving both for me and for our listeners much more insight on the topic then we've had before so I certainly do appreciate your time and your wisdom. Are they some sources that you like where our listeners can learn more?

Betsy Nichols: There actually are. There are almost – it's interesting, there are almost too many lists of metrics out there but there are lots of them. You can Google to get a lot of them but there are lists of metrics that NIST National Institute of Standards and Technology) has provided. The Center for Internet Security, the Computer Security Institute, SANS, BITS, and of course CERT are all great sources.

One other area that I think people should look at is the common vulnerability scoring system that's provided by Mitre. It provides a very nice framework that sort of divides a metric into a base score and then a score that is modified based on context and then another score, yetanother score that's modified based on temporal area. As time changes for example, is the nature of a vulnerability going to change? So that common vulnerability scoring system is good.

I also highly recommend Andrew Jacquith's book that's called *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. It's available on Amazon. In the interest of full disclosure, I was a contributor.

Julia Allen: Those are great sources and we'll certainly make sure to include links to all of them in our show notes.

Betsy Nichols: Okay, great.

Julia Allen: So again thank you so very much and I look forward to future conversations.

Betsy Nichols: Thank you very much.